NEWS
Cyber Security
Vol. 4 | Issue 2
February 2019

Welcome to the TXDPS Cyber Newsletter.

Hello everyone and welcome to this month's newsletter. To start I want to remind everyone that we are coming up on Tax season. It is also the time of year when we see an increase of scam, phishing, and malware campaigns. These campaigns can be via websites, emails, social media, or phone calls. Please be on the lookout for these scams so you don't fall victim to them. Here are a few examples to give you an idea of what to be on the lookout for.

IRS website Tax Scams / Consumer Alerts

IRS website IRS Urges Public to Stay Alert for Scam Phone Calls

TurboTax website Beware of IRS Phone Scams

YouTube video published Jul 24, 2018 Two IRS scammers arrested in Arizona

Federal Trade Commission IRS Imposter Scams

Good luck and hopefully you will not have to give extra money to the IRS this year.

Feature Highlight - Email Encryption

I was asked by our CJIS team to remind everyone about the need to encrypt sensitive data leaving the agency. I posted this in the November 2018 edition of the newsletter but want to repost it as a reminder to everyone.

Email Encryption, what is it? Email encryption involves encrypting, or disguising, the content of email messages in order to protect sensitive information from being read by anyone other than intended recipients. This is especially important when sending messages that contain sensitive, confidential and certain regulated information to recipients outside of the agency.

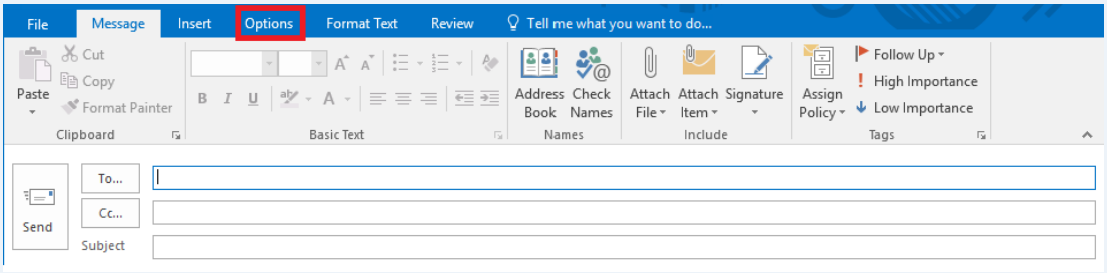
The General Manual, Chapter 26 section 26.120.00 DATA CLASSIFICATION policy (Information Resource Policy) defines sensitive, confidential and regulated data and provides examples (Chapter 26 Annexes) of each. If you have any questions concerning data classification, please contact the Cyber Risk and Vulnerability Management Team at GRP_Cyber_Risk@dps.texas.gov.

Fortunately, the feature to encrypt an email message is built into your version of Microsoft Outlook. With just a few steps, the content of your email is encrypted which gives you confidence that the intended recipient is the only person who will be able to read it. The intended recipient does not receive a traditional email within their mailbox. Instead, they receive a link to securely log into a portal where they can safely read and reply to the message. This feature is not to be overlooked as it provides an additional layer of security that prevents information from getting into the wrong hands.

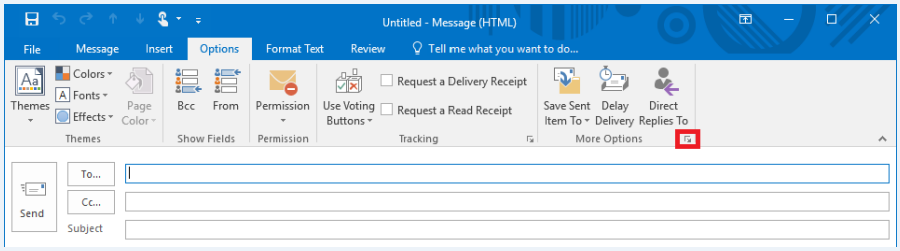
The steps provided below are for Microsoft Outlook 2016. Steps for Outlook versions 2010 and 2013 are similar but will not reflect the screenshots exactly. We will provide links to instructions for versions 2010 and 2013 at a later time.

Email Encryption

Step 1: Begin by starting a new email and click the “Options” tab



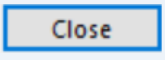
Step 2: Within the More Options section, click the icon in the right-hand corner



Step 3: Once the Properties window appears, click the “Sensitivity” drop-down menu

Step 4: Select “Confidential” from the menu list

Step 5: Click “Close”. The email is now set for encryption and will be encrypted once the message is sent



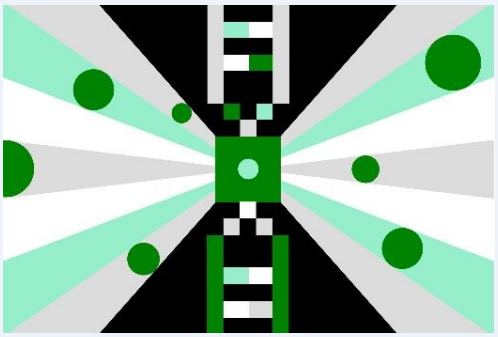
If you encounter any difficulty with encrypting emails using this process, please contact the Service Desk at 512-424-5432.

For more information on this and other topics, DPS employees can visit our SharePoint site by going to https://dpsnet.tle.dps and clicking on our Cyber Security link.

Biohackers / Ransomware

BIOHACKERS ENCODED MALWARE IN A STRAND OF DNA

(by **Andy Greenberg | 08.10.17 @ 12:00 AM**)



When biologists synthesize DNA, they take pains not to create or spread a dangerous stretch of genetic code that could be used to create a toxin or, worse, an infectious disease. But one group of biohackers has demonstrated how DNA can carry a less expected threat—one designed to infect not humans nor animals but computers.

In new research they plan to present at the USENIX Security conference on Thursday, a group of researchers from the University of Washington has shown for the first time that it's possible to encode malicious software into physical strands of DNA, so that when a gene sequencer analyzes it the resulting data becomes a program that corrupts gene-sequencing software and takes control of the underlying computer. While that attack is far from practical for any real spy or criminal, it's one the researchers argue could become more likely over time, as DNA sequencing becomes more commonplace, powerful, and performed by third-party services on sensitive computer systems. And, perhaps more to the point for the cybersecurity community, it also represents an impressive, sci-fi feat of sheer hacker ingenuity.

"We know that if an adversary has control over the data a computer is processing, it can potentially take over that computer," says Tadayoshi Kohno, the University of Washington computer science professor who led the project, comparing the technique to traditional hacker attacks that package malicious code in web pages or an email attachment. "That means when you're looking at the security of computational biology systems, you're not only thinking about the network connectivity and the USB drive and the user at the keyboard but also the information stored in the DNA they're sequencing. It's about considering a different class of threat."

Click **HERE** to read the article.

Sly criminals package ransomware with malicious ransom note

(**Malwarebytes Labs | 25 January 19**)

Ransomware continues to show signs of evolution. From a simple screen locker to a highly-sophisticated data locker, ransomware has now become a mainstream name, even if (historically), it has been around far longer than we want to look back.

Although the criminals behind ransomware campaigns are observed to be refining their approaches—from the "spray and pray" tactic to something akin to wide beam laser precision—they are also fine-tuning their targets. They can single out organizations, companies, and industries; and they can also hold cities and towns for ransom.

Ransomware has also stepped up in sophistication. Criminals have begun introducing certain forms of hybridization in their attacks, either the ransomware file itself is given capabilities outside of its type (e.g., VirRansom and Zcrypt variants that can infect files) or the entire campaign involves one or more threat vectors.

The latest in-the-wild ransomware strain discovered by a group of security researchers known as MalwareHunterTeam (MHT, for short) fits the latter.

Ransomware + phishing: a match made in heaven?

Nothing much is known about this ransomware—which some are already dubbing as CryTekk—apart from the way it applies a wily social engineering tactic to its ransom note, potentially to ensure a near 100 percent of affected parties acting on the infection and paying the ransom. The lure? An additional payment option for affected users who want to retrieve their files but don't have a cryptocurrency wallet.

Click **HERE** to read the article.

John Wick / UAE

Scam campaign camouflages as John Wick movie-based ebooks on Kindle store

(CYWARE | February 5, 2019)

- Fake ebooks with John Wick 3 cover images redirect users to third-party websites.
- Most of these links had prices ranging from £0.99 to as high as £15.25.

A new spam campaign has apparently targeted John Wick fans on Amazon's Kindle store. Miscreants have created fake ebooks in the store that resembles the third installment of the movie. When users click on these links after buying them, they will be taken to a series of third-party websites which ask for payments to view the movie.

According to Malwarebytes which uncovered this scam, these ebooks come with a price tag ranging from as low as £0.99 to around £15.25. On top of this, the fake ebooks flood the results page when users search for John Wick.

"Roughly 40 or more individual items uploaded from around January 25 to February 2, each one from a different "author." At first glance, you might think you're looking at movies, thanks to the play button icon on each image preview. The fact that each entry is called something along the lines of "John Wick 3: free movie HD" probably helps, too," wrote senior researcher Christopher Boyd from the security firm.

Click **HERE** to read more.

UAE used cyber superweapon to spy on iPhones of foes

(by **Joel Schectman** and **Christopher Bing** | **Dec 27th 2018**)

WASHINGTON (Reuters) - A team of former U.S. government intelligence operatives working for the United Arab Emirates hacked into the iPhones of activists, diplomats and rival foreign leaders with the help of a sophisticated spying tool called Karma, in a campaign that shows how potent cyber-weapons are proliferating beyond the world's superpowers and into the hands of smaller nations.

The cyber tool allowed the small Gulf country to monitor hundreds of targets beginning in 2016, from the Emir of Qatar and a senior Turkish official to a Nobel Peace laureate human-rights activist in Yemen, according to five former operatives and program documents reviewed by Reuters. The sources interviewed by Reuters were not Emirati citizens.

Karma was used by an offensive cyber operations unit in Abu Dhabi comprised of Emirati security officials and former American intelligence operatives working as contractors for the UAE's intelligence services. The existence of Karma and of the hacking unit, code named Project Raven, haven't been previously reported. Raven's activities are detailed in a separate story published by Reuters today.

The ex-Raven operatives described Karma as a tool that could remotely grant access to iPhones simply by uploading phone numbers or email accounts into an automated targeting system. The tool has limits — it doesn't work on Android devices and doesn't intercept phone calls. But it was unusually potent because, unlike many exploits, Karma did not require a target to click on a link sent to an iPhone, they said.

In 2016 and 2017, Karma was used to obtain photos, emails, text messages and location information from targets' iPhones. The technique also helped the hackers harvest saved passwords, which could be used for other intrusions.

It isn't clear whether the Karma hack remains in use. The former operatives said that by the end of 2017, security updates to Apple Inc's iPhone software had made Karma far less effective.

Lori Stroud, a former Raven operative who also previously worked at the U.S. National Security Agency, told Reuters of the excitement when Karma was introduced in 2016. "It was like, 'We have this great new exploit that we just bought. Get us a huge list of targets that have iPhones now,'" she said. "It was like Christmas."

Click **HERE** to read .

Cybercriminals / FaceTime

Cybercriminals Exploit Gmail Feature to Scale Up Attacks

(by **Jai Vijayan | 2/5/2019 @ 04:35 PM)**

Criminals are taking advantage of Gmail's 'dots don't matter' feature to set up multiple fraudulent accounts on websites, using variations of the same email address, Agari says.

Some cybercriminals are taking advantage of a long-standing feature in Google Gmail designed to enhance account security, to create multiple fraudulent accounts on various websites quickly and at scale, security vendor Agari said this week.

The feature, which some have warned about previously, basically ensures that all dotted variantions of a Gmail address belong to the same account. For example, Google treats johnsmith (at) gmail.com the same as john.smith (at) gmail.com and jo.hn.smith (at) gmail.com. An individual with johnsmith (at) gmail.com as their email address would therefore receive emails sent to *all* dotted variations of the same address.

A Google spokesperson declined to comment on the Agari research, but pointed to Google's official description of the dots feature, where Google says that the "dots don't matter" approach in Gmail ensures no one can take another person's username. "Your Gmail address is unique. If anyone tries to create a Gmail account with a dotted version of your username, they'll get an error saying the username is already taken," Google said in its post on the feature.

Click **HERE** to read more.

House Democrats want Apple to answer questions on FaceTime flaw

(by **David Shepardson | February 5, 2019**)

WASHINGTON (Reuters) - Two key U.S. House of Representatives Democrats on Tuesday asked Apple Inc Chief Executive Tim Cook, to answer questions about a privacy flaw in Apple's group video chat software after a teenager and his mother tried for days to warn the iPhone maker of the bug.

Apple said on Friday it had fixed the issue with FaceTime and said it planned to improve how it handles reports of software bugs.

House Energy and Commerce Chairman Frank Pallone and Representative Jan Schakowsky, who chairs a subcommittee overseeing consumer issues said in a letter they were "deeply troubled" over how long it took Apple to address the security flaw.

They want to know when Apple first learned of the issue, the extent to which the flaw may have compromised consumers' privacy, and if "there are other undisclosed bugs that currently exist and have not been addressed."

Apple did not immediately comment to Reuters.

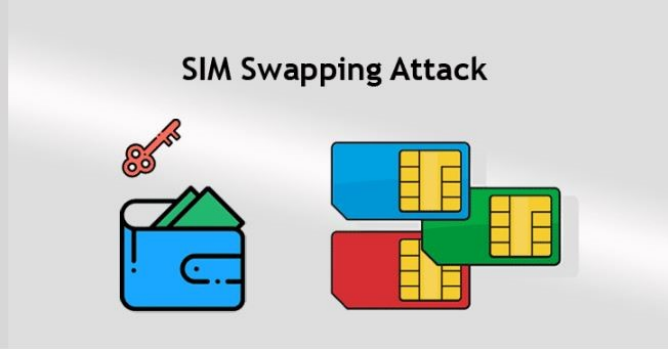
"Your company and others must proactively ensure devices and applications protect consumer privacy, immediately act when a vulnerability is identified and address any harm caused when you fail to meet your obligations to consumers," the Democrats wrote. "We do not believe Apple has been as transparent as this serious issue requires."

Click **HERE** to read more.

Sim Swapping / Vaporworms

First Hacker Convicted of 'SIM Swapping' Attack Gets 10 Years in Prison

(by **Swati Khandelwal** | **February 04, 2019**)



A 20-year-old college student who stole cryptocurrency worth more than $5 million by hijacking victims' phone numbers has pleaded guilty and accepted a sentence of 10 years in prison.

Ortiz was arrested last year on charges of siphoning millions of dollars in cryptocurrency from around 40 victims using a method commonly known as "**SIM swapping**," which typically involves fraudulently porting of the same number to a new SIM card belonging to the attacker.

In SIM swapping, attackers social engineer a victim's mobile phone provider by making a phony call posing as their target and claiming that their SIM card has been lost and that they would like to request a SIM swap.

The attackers attempt to convince the target's telecommunications company that they are the actual owner of the phone number they want to swap by providing required personal information on the target, like their SSNs and addresses, eventually tricking the telecoms to port the target's phone number over to a SIM card belonging to the attackers.

Once successful, the attackers essentially gained access to their target's mobile phone number using which they can obtain one-time passwords, verification codes, and two-factor authentication in order to reset passwords for and gain access to target's social media, email, bank, and cryptocurrency accounts.

Click **HERE** to read more.

Why vaporworms might be the scourge of 2019

(by **Marc Laliberte** | **February 5, 2019**)

Not too long ago, the WatchGuard Threat Lab predicted the emergence of vaporworms as a major new cyber threat that will affect organizations of all sizes in 2019. We coined the term to describe a new breed of fileless malware with self-propagating, wormlike properties. At the time of the initial prediction, our team was fairly sure this idea was more than conjecture, but now the advent of the vaporworm in 2019 seems to be an abject certainty.

But before I get into why and how this new threat will pick up steam this year, let's take a step back to first examine fileless attacks and how they differ from traditional malware.

The fundamentals of fileless malware

Most conventional malware variants require users to save and execute a file on their system. The file itself could be a standalone executable binary, a trojanized application, or even just a blob of instructions and data that another component loads and runs. There are many opportunities to catch traditional malware, both as it traverses the network and when it is finally saved onto a system.

Fileless malware turns everything on its head. As the name suggests, fileless malware does not save anything to the target system's storage for persistence. Instead, it leverages PowerShell and scripts, or even exploits legitimate processes to inject itself into computer memory and execute directly from there. Fileless malware is much better at covering its tracks because it doesn't leave anything behind for traditional anti-malware tools to scan.

Click **HERE** to read more.

More News

Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts

https://motherboard.vice.com/en_us/article/mbzvxv/criminals-hackers-ss7-uk-banks-metro-bank

Apple Could Drop Support for All iPhones Through iPhone 6s with iOS 13

https://news.softpedia.com/news/apple-could-drop-support-for-all-iphones-through-iphone-6s-with-ios-13-524788.shtml

U.S. wants Western tech to be used instead of Huawei kit

https://finance.yahoo.com/news/u-wants-western-tech-used-instead-huawei-kit-171830054--business.html

Google+ to Shut Down for Consumers on April 2, 2019

https://news.softpedia.com/news/google-plus-to-shut-down-for-consumers-on-april-2-2019-524768.shtml

Furious Apple revokes Facebooks entry app cert after Zuck's crew abused it to slurp private data

https://www.theregister.co.uk/2019/01/30/facebook_apple_enterprise_certificate_revocation/

New Mac malware steals cookies, cryptocurrency and computing power

https://www.helpnetsecurity.com/2019/01/31/mac-malware-steals-cookies/

Google also abused its Apple developer certificate to collect iOS user data

https://www.helpnetsecurity.com/2019/01/31/google-apple-developer-certificate/

$1.7 billion in cryptocurrency was stolen and scammed in 2018

https://www.helpnetsecurity.com/2019/01/30/stolen-cryptocurrency/

Facebook Paid Teens $20 to Install 'Research' App That Collects Private Data

https://thehackernews.com/2019/01/facebook-research-app.html

Police Shut Down xDedic—An Online Market for Cyber Criminals

https://thehackernews.com/2019/01/cyber-criminal-marketplace.html

Crims use steganography to stash bad code in ads

https://www.theregister.co.uk/2019/01/24/mac_steganography_malware/

</Closing Comments>

User Suggested:

We had several great articles suggested by users for this month's newsletter. I strongly encourage everyone to read them. I've listed the user who submitted followed by the articles they submitted.

Deborah Wright:

- https://www.irishtimes.com/business/technology/mondelez-sues-zurich-over-100m-cyberhack-insurance-claim-1.3753475
- https://threatpost.com/cisco-critical-vulnerability-patch/140726/
- http://www.scmagazine.com/home/network-security/microsoft-updates-brick-windows-7-devices/
- https://techcrunch.com/2019/01/29/facebook-project-atlas/?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioscodebook&stream=technology
- https://www.wired.com/story/collection-leak-usernames-passwords-billions/

Stephen "Doc" Petty

- https://www.forbes.com/sites/thomasbrewster/2019/01/16/massive-oklahoma-government-data-leak-exposes-7-years-of-fbi-investigations/#3620927a6e11
- https://www.theinquirer.net/inquirer/news/3069445/outlook-mobile-app-now-safe-enough-to-be-used-by-pentagon

SGT Lane Tippett

- https://nypost.com/2019/01/11/employees-at-amazons-ring-have-been-spying-on-customers/

Special Agent Erich Neumann

- https://www.bleepingcomputer.com/news/security/android-apps-steal-banking-info-use-motion-sensor-to-evade-detection/

Wishes to remain unnamed

- https://www.foxnews.com/tech/hacked-nest-camera-warned-of-north-korean-missile-attack-family-says

---

Thank you everyone for taking the time out of your day to read the newsletter. I hope you found this month's newsletter informative, interesting, and useful. Remember, you can only defend yourself against threats when you are knowledgeable about the threats. I realize cybersecurity is not the most liked topic, but it is important to understand the dangers you and your family face when being online and how your actions and the actions of others can affect the Agency. Knowing about cyber dangers are all part of Cybersecurity Awareness Continuation Training. Everyone in the Agency has to take Cybersecurity Awareness training every two years, but the learning does not end when the online training is over. My hope is this newsletter provides a little more up-to-date information about Cybersecurity as well as making it a little more enjoyable than watching generic training videos online. Feedback on how to improve the newsletter is always appreciated, so feel free to email me with suggestions. If possible, I will implement them in future editions.

As I mentioned above, everyone has to take the online training every two years. I send out notifications monthly to people when it is time for their retraining. If you know you are coming up on your two year mark, please be on the lookout for the email. If you are unsure, feel free to email me and I will let you know when you are due retraining.

As a reminder, feel free to share this newsletter with friends and family. The better educated everyone is on cyber issues the safer everyone is. You can see previous issues of the website at this public facing DPS site: http://www.dps.texas.gov/InformationTechnology/Cyber/index.htm

In closing, hope you enjoyed the newsletter and good luck with the Cyber Challenge on the next page. And as always, **THANK YOU FOR YOUR CYBER VIGILANCE.**

Kirk

Cyber Challenge

Last Month's Challenge

Here are the people who completed last month's challenge along with the answers:

Erich Neumann at 1515 on 8 January	Deborah Wright at 1520 on 8 January	Jimmy Ferrer at 1523 on 8 January
Clifford Dickerson at 1532 on 8 January	Jared Crouse at 1535 on 8 January	Dylan Barnes at 1549 on 8 January
Matthew Morgan at 1557 on 8 January	Faye Krueger at 1629 on 8 January	Stephen Bell at 1707 on 8 January
Jaelyn Edwards at 0900 on 9 January	Michael Manke at 1027 on 10 January	Carla Bell at 1203 on 10 January
Jessica Jaramillo at 1150 on 17 January	Joanna Morgan at 1332 on 30 January	

Here are last month's questions with answers:

1. I am the art of manipulating people so they give up confidential information. The type of information varies but the individuals targeted are usually trying to trick you into giving them your passwords, bank information, access your computer to install malicious software, etc. What am I? **Social Engineering**
2. I am an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to prove their identity. What am I? **2 Factor or Multi-Factor**
3. SSBhbSB0aGUgZnJhdWR1bGVudCBhdHRlbXB0IHRvIG9idGFpbiBzZW5zaXRpdmUgaW5mb3JtYXRpb24gc3VjaCBhcyB1c2VybmFtZXMsIHBhc3N3b3JkcyBhbmQgY3JlZGl0IGNhcmQgZGV0YWlscyBieSBkaXNndWlzaW5nIGFzIGEgdHJ1c3R3b3J0aHkgZW50aXR5IGluIGFuIGVsZWN0cm9uaWMgY29tbXVuaWNhdGlvbi4gIFdoYXQgYW0gST8= **This needs to be converted from Base64 encoding to Text. When you do that you get this: "I am the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication. What am I?" The answer is Phishing**
4. 01001001 00100000 01100001 01101101 00100000 01110011 01101111 01100110 01110100 01110111 01100001 01110010 01100101 00100000 01110100 01101000 01100001 01110100 00100000 01101001 01110011 00100000 01101001 01101110 01110100 01100101 01101110 01100100 01100101 01100100 00100000 01110100 01101111 00100000 01100100 01100001 01101101 01100001 01100111 01100101 00100000 01101111 01110010 00100000 01100100 01101001 01110011 01100001 01100010 01101100 01100101 00100000 01100011 01101111 01101101 01110000 01110101 01110100 01100101 01110010 01110011 00100000 01100001 01101110 01100100 00100000 01100011 01101111 01101101 01110000 01110101 01110100 01100101 01110010 00100000 01110011 01111001 01110011 01110100 01100101 01101101 01110011 00101110 00100000 00100000 01001001 00100000 01100011 01101111 01101101 01100101 00100000 01101001 01101110 00100000 01101101 01100001 01101110 01111001 00100000 01100110 01101111 01110010 01101101 01110011 00101110 00100000 00100000 01010111 01101000 01100001 01110100 00100000 01100001 01101101 00100000 01001001 00111111 **This needs to be converted from Binary encoding to Text. When you do that you get this: "I am software that is intended to damage or disable computers and computer systems. I come in many forms. What am I?" The answer is Malware**
5. 49 20 61 6d 20 61 20 74 79 70 65 20 6f 66 20 6d 61 6c 69 63 69 6f 75 73 20 73 6f 66 74 77 61 72 65 20 64 65 73 69 67 6e 65 64 20 74 6f 20 62 6c 6f 63 6b 20 61 63 63 65 73 73 20 74 6f 20 61 20 63 6f 6d 70 75 74 65 72 20 73 79 73 74 65 6d 20 75 6e 74 69 6c 20 61 20 73 75 6d 20 6f 66 20 6d 6f 6e 65 79 20 69 73 20 70 61 69 64 2e 20 20 57 68 61 74 20 61 6d 20 49 3f **This needs to be converted from Hexadecimal to Text. When you do that you get this: "I am a type of malicious software designed to block access to a computer system until a sum of money is paid. What am I?" The answer is Ransomware.**

This month's challenge is on the next page. Remember, if you have difficulties solving the challenges you can always email me for hints.

Cyber Challenge

This Month's Challenge

To answer this month's Cyber Challenge questions you will first have to decode them to get the questions.

While there are other types of encoding, the ones most often used with computers are binary, hexadecimal and base64. You can find out more information about each of them by clicking the links. However, that does not mean what is below will be one of those encodings I listed.

1. 127 150 157 040 163 141 151 144 040 042 125 156 145 161 165 151 166 157 143 141 154 154 171 054 040 164 150 151 163 040 160 162 157 166 145 163 040 156 157 164 040 157 156 154 171 040 150 141 166 145 040 143 141 164 163 040 164 141 153 145 156 040 157 166 145 162 040 164 150 145 040 151 156 164 145 162 156 145 164 040 142 165 164 040 156 157 167 040 164 150 145 040 157 146 146 163 150 157 162 145 040 164 141 170 040 150 141 166 145 156 040 155 141 162 153 145 164 040 164 157 157 041 042
2. ␣↑↕ ▽⇨↓⇦ ↑⇉↕^ ▷↓◀↑↕▶◀ ▽⇨⇨▶△↓◀◢ ↴ ⇉⇔◀⇨△⇔⇨◀ ↕← ^↑△⇨⇨◀▽↓↴
3. n fr fs fiafshji, rtizqfw gfspnsl ywtofs ymfy uwnrfwnqd kzshyntsx fx f itbsqtfijw tw iwtuujw tk tymjw gfspnsl ywtofsx. n fr frtsl ymj rtxy htxyqd fsi ijxywzhynaj rfqbfwj fkkjhynsl xyfyj, qthfq, ywngfq, fsi yjwwnytwnfq (xqyy) ltajwsrjsyx, fsi ymj uwnafyj fsi uzgqnh xjhytwx. bmfy fr n?
4. 4920616d2074686520747970652066207261e736f6d7761726520746861742068697420416d73204d656d6f7269616c20486f73706974616c20696e2044656361746f722c20496e6469616e61206f6e203131204a616e756172792032303138e20205768617420616d20493f
5. 

Good Luck with the challenge. Make sure and email me your answers or if you need a hint to solve them.

Kirk.